UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/306,227	05/06/1999	ROY CALLUM	042390.P6761	3173

7590 03/26/2003

CHARLES A MIRHO INTEL CORPORATION
BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
12400 WILSHIRE BOULEVARD
7TH FLOOR
LOS ANGELES, CA 90025

EXAMINER	
REVAK, CHRISTOPHER A	

ART UNIT	PAPER NUMBER
2131	4

DATE MAILED: 03/26/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/306,227	CALLUM, ROY
	Examiner	Art Unit
	Christopher A. Revak	2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-15 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-15 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

Specification

1. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 250 words. It is important that the abstract not exceed 250 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

It is noted by the examiner that the abstract should be in the form of a single paragraph, appropriate correction is required.

Claim Objections

2. Claim 2 is objected to because of the following informalities: In claim 2, it is recited of "comprises one of an encryption **of** decryption operation" which appears to read "one of encryption **or** decryption operation" as is recited in claim 5. Appropriate correction is required.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless --
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), but another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1,2, and 4-6 are rejected under 35 U.S.C. 102(e) as being anticipated by Hardy et al.

As per claims 1 and 4, it is shown in Figure 1 of Hardy et al of an operation unit adapted to perform a circuit operation in a plurality of state vectors (rounds)(col. 3, lines 11-19). The encryption algorithm is adapted to generate a unique set of state vectors at various points in the execution of encryption algorithms and the state vectors (rounds) are used to inform the state monitor that specific sections of the selected software encryption algorithm have been executed (col. 3, lines 27-34). A state monitor compares the state vectors with predetermined (reference value identifying the correct value) state vectors (col. 3, lines 44-50). A comparator checks the operations so that they fall between a minimum and maximum threshold value (predetermined range of operating conditions)(col. 4, lines 1-4). A disablement signal is produced causing the flow of cipher text to stop when there is a miscomparison of the data (col. 12, lines 30-36).

As per claim 2, it is disclosed by Hardy et al that the circuit operation includes encryption (col. 2, lines 13-16).

As per claim 5, Hardy et al recites of generating a state vector (round) and making it available to the state monitor. A key (signal) is used for the encryption algorithm (col. 6, lines 10-19). It is taught that the circuit operation includes encryption (col. 2, lines 13-16).

As per claim 6, Hardy et al discloses of key (signal) which is used for the encryption algorithm (col. 6, lines 10-19). The examiner asserts that a first clock signal is used since the teachings of Hardy et al perform the monitoring based on normal operating conditions.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 3,7-9, and 11-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hardy et al in view of Curiger et al.

As per claims 3 and 7, Hardy et al recites of generating a state vector (round) and making it available to the state monitor. A key (signal) is used for the encryption algorithm (col. 6, lines 10-19). The examiner asserts that a first clock signal is used since the teachings of Hardy et al perform the monitoring based on normal operating conditions. The teachings of Hardy et al are silent in disclosing of providing a subsequent clock signal. It is disclosed by Curiger et al of known techniques in the prior art whereby an increased frequency (subsequent clock signal) is

applied to an integrated circuit (col. 1, lines 34-37). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply means to detect different clocking signals. Curiger et al recites motivation for this concept by reciting that increased frequency (subsequent clock signals) can cause a circuit to operate improperly and calculation errors may result (col. 1, lines 34-38). The detection of this change of clock signals would have been beneficial to the teachings of Hardy et al as a means to ensure that the encryption operations are properly computed as is taught by Curiger et al.

As per claims 8 and 13, it is shown in Figure 1 of Hardy et al of an operation unit adapted to perform a circuit operation in a plurality of state vectors (col. 3, lines 11-19). The encryption algorithm is adapted to generate a unique set of state vectors at various points in the execution of encryption algorithms and the state vectors are used to inform the state monitor that specific sections of the selected software encryption algorithm have been executed (col. 3, lines 27-34). A state monitor (sampling unit) compares the state vectors with predetermined state vectors (stored in memory)(col. 3, lines 44-50). A comparator (analytical unit) checks the operations so that they fall between a minimum and maximum threshold value (col. 4, lines 1-4). A disablement signal is produced causing the flow of cipher text to stop when there is a miscomparison of the data (col. 12, lines 30-36). The examiner asserts that a first frequency sample is used since the teachings of Hardy et al perform the monitoring based on normal operating conditions. The teachings of Hardy et al are silent in disclosing of applying a second frequency. The teachings of Curiger et al disclose of increasing an input clock frequency (second frequency sample) in order to stress the

circuitry (col. 4, lines 15-19). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply different frequency samples in order to test the circuitry for proper operations. Curiger et al recites motivation for this concept by reciting that increased frequency (subsequent clock signals) can cause a circuit to operate improperly and calculation errors may result (col. 1, lines 34-38). The detection of this change of clock signals would have been beneficial to the teachings of Hardy et al as a means to ensure that the encryption operations are properly computed as is taught by Curiger et al.

As per claims 9 and 14, Hardy et al discloses of a counter which counts the tasks (oscillations) which are performed (col. 11, lines 17-19). Curiger et al is relied upon for the disclosure of a second frequency. It is disclosed by Curiger et al of an oscillator which increases the frequency (col. 5, lines 1-6).

As per claim 11, it is taught by Hardy et al of subtracting (by a subtractor) the differences of the circuit performance levels (col. 8, lines 42-44). The teachings of Curiger et al are relied upon for the disclose of multiple frequency samples.

As per claim 12, Hardy et al disclose of a (magnitude) comparator which checks the operations so that they fall between a minimum and maximum threshold value (col. 4, lines 1-4). The teachings of Curiger et al are relied upon for the disclose of multiple frequency samples.

As per claim 15, the examiner asserts that a first frequency sample is used since the teachings of Hardy et al perform the monitoring based on normal operating conditions at the start

of circuit operations. Curiger et al is relied upon for increasing an input clock frequency (second frequency sample) in order to stress the circuitry (col. 4, lines 15-19).

7. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hardy et al in view of Curiger et al in further view of Mertel et al.

The teachings of Hardy et al disclose of a counter, but is silent in disclosing that the counter is a Johnson counter. It is disclosed by Mertel et al of a counter which is a Johnson counter (col. 5, lines 5, lines 30-31). I would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply a Johnson counter as a specific counter. Mertel et al discloses the benefits of a Johnson counter by reciting that it is used to identify specific master clock cycles and initiate various actions. The advantage of this particular type of counter is that is does not require numerous decode gate to identify cycles which saves hardware (col. 5, lines 6-12). It is obvious that the teachings of Hardy et al would have benefitted from the use of a Johnson counter as per the advantages recited by Mertel et al.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Thiriet, U.S. Patent 6,101,254

Albert et al, U.S. Patent 5,870,469

Mishra, U.S. Patent 5,844,823

Likens et al, U.S. Patent 5,608,798

Butter et al, U.S. Patent 5,432,848

Ogawa, U.S. Patent 4,962,352

Wang et al, "On the Hardware Design for DES Cipher in Tamper Resistant Devices against Differential Fault Analysis"

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher Revak whose telephone number is (703) 305-1843. The examiner can normally be reached on Monday-Thursday from 6:30 am to 4:00 pm. The examiner can also be reached on alternate Fridays from 6:30 am to 3:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail Hayes, can be reached on (703) 305-9711. The fax phone number for the organization where this application or proceeding is assigned as follows:

for After-Final Communications:	(703) 746-7238;
for Official Communications:	(703) 746-7239;
for Non-Official Communications:	(703) 746-7240.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

CR

March 23, 2003

GAIL HAYES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100